IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA	)	DOCKET NO. 3:25-CR-76-MOC
	)	
v.	)	**BILL OF INFORMATION**
	)	
Nicholas Moses, a/k/a "scrublord"	)	18 U.S.C. § 371

THE UNITED STATES ATTORNEY CHARGES:

At the specified times and at all relevant times:

Overview

1. At all times relevant to this Information, Nicholas MOSES, a/k/a "scrublord," the defendant, operated a computer malware program known as SmokeLoader. MOSES deployed the malware as a means to harvest personal information and passwords from victims without the knowledge of the owners of the victim computers.

2. Thousands of computers around the world have been infected with the SmokeLoader malware by MOSES and over 65,000 victims have had their personal information and passwords stolen by MOSES.

Background and Definitions

3. "Malware" is a term for a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, and perform other unauthorized actions on computer systems. Common examples of malware include viruses, ransomware, worms, keyloggers, and spyware.

4. "Infostealers" are part of a family of malware generally known as remote access trojans, or "RATs." Infostealers or RATs function primarily through gaining administrative access to a computer without the user's permission, whereafter they perform various illicit functions on an infected device. Infostealers typically feature functions that include, but are not limited to, the theft of financial information, as well as the theft of saved username and password combinations for websites and other services.

5. "SmokeLoader" is a form of malware that functions as a trojan virus, which allows users to gain unauthorized access to a victim computer. After infecting a computer,

SmokeLoader attempts to install additional malware on the device. One such type of additional malware used by the SmokeLoader platform is an infostealer. SmokeLoader was designed to perform these and other functions without alerting the users and/or owners of the infected computer in order to avoid detection.

6. A "command and control server" was a centralized computer that issued commands to remotely connected computers. "Command and Control" ("C2") infrastructure consisted of servers and other technical infrastructure that issued commands to control malware.

7. Company 1 was an FDIC-insured financial institution with a headquarters located in Charlotte, North Carolina, within the Western District of North Carolina.

Count One

Conspiracy to Commit Fraud and Related Activity in Connection with Computers
(18 U.S.C. § 371 (18 U.S.C. §§ 1030(a)(2)(C) and (a)(4)))

8. The United States Attorney re-alleges and incorporates by reference herein paragraphs 1 through 7 of this Bill of Information.

9. From at least in or about January 2022, the exact date being unknown to the United States Attorney, until in or about May 2023, within the Western District of North Carolina and elsewhere, the defendant,

NICHOLAS MOSES a/k/a "scrublord,"

did knowingly combine, conspire, confederate, and agree with others known and unknown to the United States Attorney, to commit offenses against the United States, that is: intentionally access a computer without authorization and thereby obtain information from any protected computer for the purpose of commercial advantage and private financial gain, and aid, abet, procure, and include the same; and knowingly and with intent to defraud, access a protected computer, without authorization, and by means of such conduct further the intended fraud and obtaining something of value, specifically, financial and other data from multiple computers, and aid, abet, procure, and induce the same, in violation of Title 18 United States Code, Sections 1030(a)(2)(C), (a)(4), (c)(2)(B)(i), and (c)(3)(A).

Purpose of the Conspiracy

10. It was the purpose of the conspiracy for defendant MOSES and other conspirators to unlawfully enrich themselves by: (a) deploying infostealer malware through SmokeLoader that would, when executed, steal data from victim computers; (b) maintaining digital infrastructure, including C2 and storage servers to deliver the malware

as well as store the stolen victim data; and (c) receiving the stolen data from victim computers.

Manner and Means of the Conspiracy

11. The manner and means by which defendant MOSES sought to accomplish the purpose of the conspiracy included, among other things:

a. MOSES deployed malware via SmokeLoader, which was designed to steal data from victim computers, for the purpose of commercial advantage and private financial gain. MOSES deployed the SmokeLoader malware as early as January 2022.

b. MOSES maintained and operated a C2 server located in the Netherlands to deploy the malware and receive the stolen data from victim computers, including personal information and account credentials and passwords.

c. MOSES used SmokeLoader to steal any available online account names and passwords, and other valuable digital data from the victim computers. The stolen data was sent to a server controlled by MOSES.

d. MOSES retained a copy of the stolen data on his personal devices. MOSES's C2 server and personal devices contained stolen data from approximately 65,000 victims.

e. The information could either be sold in a dark-web marketplace or other online cybercrime forum to those who would exploit it or be exploited directly by MOSES.

Overt Acts

12. In furtherance of the conspiracy and to effect its unlawful objects, defendant MOSES and other conspirators committed and caused to be committed the following overt acts in the Western District of North Carolina and elsewhere:

a. On or about January 2, 2022, MOSES purchased a virtual private server located in the Netherlands to host the SmokeLoader malware as a C2 and to receive the stolen victim data.

b. On or about October 30, 2022, MOSES received an invoice from the proxy service which maintained his virtual private server for the SmokeLoader C2. On the same date, MOSES paid approximately 10.00 EUR to maintain the server, which

was reflected in an "Invoice Payment Confirmation" email he received shortly thereafter.

c. On or about December 2, 2022, MOSES created a file on his home computer which contained the stolen data from over 8,000 victim computers.

d. Between about December 2, 2022, and about January 5, 2023, MOSES created files on the server he maintained and operated in the Netherlands which contained the stolen data from over 65,000 victim computers.

e. On or about December 2, 2022, MOSES created files on his home computer and his virtual private server located in the Netherlands which contained at least 12 sets of stolen usernames and passwords of victims for their online bank accounts at Company 1.

f. On or about November 30, 2022, MOSES participated in an online chat session during which he provided the usernames and passwords for victim accounts with multiple video on-demand streaming services, which were acquired through the SmokeLoader infostealer.

g. On or about December 11, 2022, MOSES participated in an online chat session during which he stated that he had acquired "over half a million stealer logs" and that he sold the stolen victim credentials and passwords or "$1-5 each."

h. On or about December 16, 2022, MOSES participated in an online chat session during which he sent a screenshot of his SmokeLoader interface from his server in the Netherlands, which reflected a database of 619,763 files containing stolen victim data.

i. On or about February 4, 2023, MOSES logged into the Dutch server that hosted the SmokeLoader malware and the victims' stolen data.

j. On or about March 17, 2023, MOSES accessed the stolen victim data on his home computer.

All in violation of Title 18, United States Code, Section 371 and Sections 1030(a)(2)(C), (a)(4), (c)(2)(B)(i), and (c)(3)(A).

NOTICE OF FORFEITURE

Notice is hereby given of 18 U.S.C. §§ 982 and 1030(i) and 28 U.S.C. § 2461(c). Under Section 2461(c), criminal forfeiture is applicable to any offenses for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all

specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to proceeds by § 981(a)(1)(C). The following property is subject to forfeiture in accordance with sections 982 and 1030(i) and/or section 2461(c):

a. all property which constitutes or is derived from proceeds of the violations set forth in this Bill of Information;

b. all property used or intended to be used to commit the violations alleged in this Bill of Information, and

c. in the event that any property described in (a) or (b) cannot be located or recovered or has been substantially diminished in value or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant, to the extent of the value of the property described in (a) and (b).

The following property is subject to forfeiture on one or more of the grounds stated above:

a. a black Phanteks computer tower, serial number C14061000032;

b. a one terabyte NVMe Intel SSDPELNW01 hard drive, serial number BTNR04851SMT1P0B;

c. a four terabyte Western Digital WD40EFAX-68JH4N1 hard drive, serial number WD-WX22D90LT2AA;

d. a 20 terabyte Exos X20 hard drive, serial number ZVTO45QA; and

e. a two terabyte Seagate Barracuda ATA ST2000DM006-2DM164 hard drive, serial number Z4Z99VFD.

RUSS FERGUSON
UNITED STATES ATTORNEY

MATTHEW T. WARREN
ASSISTANT UNITED STATES ATTORNEY

For RYAN K.J. DICKEY
SENIOR COUNSEL
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION